

(19)



(11)

EP 3 726 406 B1

(12)

EUROPEAN PATENT SPECIFICATION

(45) Date of publication and mention of the grant of the patent:

06.04.2022 Bulletin 2022/14

(51) International Patent Classification (IPC):

G06F 21/31 ^(2013.01) **H04L 29/06** ^(2006.01)

(21) Application number: **20159902.4**

(52) Cooperative Patent Classification (CPC):

G06F 21/31; H04L 63/083; H04L 63/205;

G06F 2221/2131; G06F 2221/2135

(22) Date of filing: **27.02.2020**

(54) PREVENTING ACCOUNT LOCKOUT THROUGH REQUEST THROTTLING

VERHINDERUNG VON KONTENSPERREN DURCH ANFRAGENDROSSELUNG

PRÉVENTION DE VERROUILLAGE DE COMPTE PAR ÉTRANGLEMENT DE REQUÊTE

(84) Designated Contracting States:

**AL AT BE BG CH CY CZ DE DK EE ES FI FR GB
GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO
PL PT RO RS SE SI SK SM TR**

(30) Priority: **15.04.2019 US 201962834274 P**

19.02.2020 US 202016795359

(43) Date of publication of application:

21.10.2020 Bulletin 2020/43

(73) Proprietor: **Pulse Secure, LLC**

San Jose CA 95134 (US)

(72) Inventors:

- **KAHN, Clifford E.**
Westford, MA Massachusetts 01886 (US)
- **K, Siva Kumar**
Virat Nagar (IN)
- **LITTRELL, Brett**
Fremont, CA California 94538 (US)

(74) Representative: **Hepworth Browne**

15 St. Pauls Street
Leeds LS1 2JG (GB)

(56) References cited:

US-A1- 2004 093 519 US-A1- 2006 130 140
US-A1- 2017 208 075

EP 3 726 406 B1

Note: Within nine months of the publication of the mention of the grant of the European patent in the European Patent Bulletin, any person may give notice to the European Patent Office of opposition to that patent, in accordance with the Implementing Regulations. Notice of opposition shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

Description

RELATED APPLICATIONS

[0001] This application is related to U.S. Provisional Patent Application No. 62/834,274, filed April 15, 2019, the content of which may be of interest to the skilled reader.

TECHNICAL FIELD

[0002] This disclosure relates to computer networks, and more particularly, to user authentication for computer networks.

BACKGROUND

[0003] Computing devices perform user authentication to ensure that only authorized users are permitted access to various computer resources. Typically, authentication includes a user providing a username and password. A computing device receives the username and password and determines whether the received username and password match stored data representing a previously established username and password. For example, the computing device may include a database that stores a hash of the password associated with the username, which acts as a key entry in a table.

[0004] Malicious users have developed strategies to attempt to gain unauthorized access to computing devices. One malicious attack includes a dictionary attack, in which a malicious user submits a large number of passwords associated with a particular username, where the large number of passwords is selected from a dictionary of commonly used passwords. To thwart such an attack, many authentication systems impose a lockout on user accounts for which too many incorrect password attempts are made. In particular, authentication systems lock a user's access for a period of time if more than a configurable number of failed password attempts are made to access services for which access control is supported by the authentication sources.

[0005] In some examples, an identity provider (IDP) communicates a user's password to an authentication source when the user attempts to access a service that is controlled or hosted by a service provider (SP). Upon receiving a failed authentication message from the authentication source in response to the IDP sending a bad password, i.e., a password that does not match the user's password recorded by the authentication source, the IDP may re-transmit an authentication request that includes the bad password to the authentication source multiple times. In some cases the IDP re-transmits a bad password to the authentication source when the SP re-transmits an authentication request including the bad password to the IDP. After receiving the bad password, or multiple different bad passwords, multiple times, the authentication source locks the user's access.

[0006] In some configurations a user's access can only be unlocked through administrator intervention or by a user providing additional information and, in some cases, resetting their password. An authentication source may lock a user's access in response to legitimate security threats, for example in response to a brute force hacking attempt whereby a malicious user attempts to gain access to a resource by iteratively guessing a user's password and submitting multiple different guessed passwords. However, an authentication source may also lock a user's access in response to more benign password failures, for example, when a user changes a password registered with the authentication source but fails to update the corresponding password stored on a user device. Another benign password failure may occur when the user changes both the authentication source password and the user device password, but the update to the authentication source password is not fully implemented by the authentication source prior to the user making a resource access attempt.

[0007] US 2017/208075 A1 discusses a "smart lockout" arrangement.

[0008] US 2006/130140 A1 discusses a system and method for protecting a server against denial of service attacks.

[0009] US 2004/093519 A1 discusses a network protecting authentication proxy.

SUMMARY

[0010] The invention is defined in the appended claims. In general, this disclosure describes techniques for preventing lockout of a user's account for benign password attempts. The techniques of this disclosure may be used to distinguish between true attacks and benign password failures. The techniques of this disclosure may therefore be used to prevent account lockouts in response to benign password failures while maintaining protection against truly malicious activity.

[0011] An example method includes determining that a received first password for a user account is not valid for the user account. The method also includes, in response to determining that the first password is not valid, incrementing a lockout counter associated with the user account. Additionally, the method includes determining that a received second password for the user account is the same as the first password, and in response to determining that the second password is the same as the first password, preventing incrementing of the lockout counter.

[0012] An example server provides a single sign on service. The server includes memory storing an attempt table and a processor. The server, in response to receiving a first password for a user account, forwards the first password to an authentication device. The server determines that the first password is not valid for the user account. The server stores the first password in association with the user account in the attempt table. In re-

sponse to receiving a second password for the user account, the server determines whether the second password matches the first password. When the second password does not match the first password, the server forwards the second password to the authentication device.

[0013] An example transitory or non-transitory computer readable medium comprises instructions that, when executed, cause a server to, in response to receiving a first password for a user account, forward the first password to an authentication device, determine that the first password is not valid for the user account, and store the first password in association with the user account in the attempt table. The instructions also cause the server to, in response to receiving a second password for the user account, determine whether the second password matches the first password, and when the second password does not match the first password, forward the second password to the authentication device.

[0014] The details of one or more examples are set forth in the accompanying drawings and the description below. Other features, objects, and advantages will be apparent from the description and drawings, and from the claims.

BRIEF DESCRIPTION OF DRAWINGS

[0015]

FIG. 1 is a block diagram illustrating an example network including user devices, service provider devices, an identity provider device, and an authentication device, which may be configured to perform the techniques of this disclosure.

FIG. 2 is a block diagram illustrating an example of the network of FIG. 1 configured to perform the techniques of this disclosure in a first scenario.

FIG. 3 is a block diagram illustrating an example of the network of FIG. 1 configured to perform the techniques of this disclosure in a second scenario.

FIG. 4 is a block diagram illustrating an example of the network of FIG. 1 configured to perform the techniques of this disclosure in a third scenario.

FIG. 5 is a block diagram illustrating an example of the network of FIG. 1 configured to perform the techniques of this disclosure in a third scenario.

FIG. 6 is a flowchart illustrating an example method for performing techniques of this disclosure.

FIG. 7 is a flowchart illustrating an example of a method for performing techniques of this disclosure.

DETAILED DESCRIPTION

[0016] Benign password failures happen when a true user of an account attempts to log into the account but supplies the incorrect password. For example, a user may change a password registered with the authentication source but fail to update the corresponding password stored on a user device. As another example, benign

password failure may occur when the user changes both the authentication source password and the user device password, but user device attempt to access the account before the authentication source password is implemented by the authentication source. One of these example failures can cause multiple requests with the wrong password to be sent to the authentication source in a short period of time which in turn may trigger an account lock. For example, a client on a user's mobile device and a client on a user's laptop may attempt to access a protected network resource (such as an email server) in a short period of time. Thus, these failures may cause a user to be locked out of their account until some intervention, such as resetting the password or manually unlocking the account by an administrator. These interventions can use network resources to resolve and cause frustration to a user.

[0017] As described below, authentication requests are filtered (sometimes referred to as "throttled") before reaching an authentication device to distinguish between malicious attacks and benign password failures. The system reduces and/or eliminates benign password failures that result in an account lock, while allowing malicious attacks to trigger the defensive measures of the authentication device. Users registers usernames and passwords with the authentication source. An identity provider device provides an authentication service for authenticating users and is communicatively coupled to the authentication source. The identity provider device receives username and passwords from service providers that received them from user devices. The identity provider device then requests authentication from the authentication service. The authentication service communicates either a verification message or a fail to verify message (sometimes referred to as a "failure message") to the identity provider device based on the comparison. In one attack mitigation strategy, when a failure message is generated, the authentication service may increment a lockout counter. When the lockout counter satisfies (e.g., is greater than or equal to, etc.) a failure threshold, the authentication service may lockout the account until an intervention is taken.

[0018] The received message is forwarded to the service provider that requested the authentication. The identity provider device prevents the authentication service from, for example, incrementing the lock counter because of the same failed password. In response to receiving a failure message, the identity provider device stores the password associated with the failure. The failed password is stored associated with the username on a failure table as, for example, a one-way hash of the failed password. In some examples, the failed password is stored for a limited amount of time (e.g., thirty seconds, a minute, two minutes, etc.). Additionally, in some examples, the failure table may store multiple failure passwords such that the system is more user error tolerant. Upon receiving another request for authentication with the same username, the identity provider device com-

compares the accompanying password (e.g., a one-way hash of the accompanying password, etc.) to the failed password (e.g., a one-way hash of the failed password, etc.) stored in the database. If the two passwords match, the identity provider device does not forward the authentication request to authentication service. If the two passwords do not match, the identity provider device forwards the authentication request to authentication service.

[0019] FIG. 1 is a block diagram illustrating an example network 100 including user devices 102A and 102B (collectively referred to as "user device 102"), service provider (SP) devices 104A and 104B (collectively referred to as "SP device 104"), identity provider (IDP) device 106, authentication device (AD) 108, attempt table 110, and user credentials database 112, which may be configured to perform the techniques of this disclosure. A user may use multiple user devices 102 to access services provided on SP 104. For example, the same user may use each of a desktop computer at an office, a desktop computer at home, a laptop, a tablet, and a smart phone. Such devices may each access a variety of SP devices 104 for the same or different services, e.g., based on a location of the user and the user device at a particular time when the user is accessing the services.

[0020] In general, SP device 104 provides one or more services. Such services may include various software applications (e.g., email, word processing, spreadsheet programs, database programs, presentation programs, or the like), network services such as online shopping services, media streaming services (e.g., audio and/or video streaming), or the like. Users access the services provided by SP device 106 using one or more user devices 102. For example, a user may access a Software as a Service (SaaS) service operating on SP device 106A using user device 102A (e.g., a smartphone, a tablet, a laptop, etc.) and user device 102B (e.g., a desktop, a laptop, a workstation, etc.). SP device 104 provides such services to authorized users that provide valid credentials (e.g., a username and password, etc.). These services may require the user device 102 to provide credentials from time-to-time (e.g., when logging into the service after disconnecting, periodically while connected, etc.). For example, a service may require authorization when the user device 102 initially connects and may require a renewed authorization every 15 minutes thereafter. The authentication service may provide single sign on (SSO), in which a user of user device 102 may provide a single user identifier (ID) (e.g., a username, etc.) and password to gain access to a variety of services provided by, e.g., one or more SP devices 104. In such a manner, SP devices 104 may request multiple authorization for the same credentials over a relatively short period of time.

[0021] In the illustrated example, the SP device 104 is communicatively coupled to IDP device 106. IDP device 106 provides authentication services for authenticating users of the SP device 104, such as a user of user device 102. Additionally or alternatively, in some example, SP device 104 may itself provide an authentication service

for authenticating users. IDP device 106 acts as an intermediary between the authorization requests sent by SP device 104 and authentication device 108. The authentication service of IDP 106 may include an authentication, authorization, and accounting (AAA) service. User device 102, SP device 104, and IDP device 106 may be configured according to one or more of a variety of authentication services and authentication protocols, such as Remote Authentication Dial-In User Service (RADIUS), Diameter, Lightweight Directory Access Protocol (LDAP), Security Assertion Markup Language (SAML), Open Authorization (OAuth), OAuth 2.0, Terminal Access Controller Access-Control System Plus (TACACS+), Kerberos, or the like. In some examples, user device 102 (or another device between user device 102 and SP device 104, such as a gateway device, not shown in FIG. 1) may execute an Enhanced Client or Proxy (ECP) profile, e.g., of SAML.

[0022] In the illustrated example, IDP device 106 is communicatively coupled to authentication device 108. In general, to authenticate a user of user device 102, IDP device 106 receives a username and password for the user via SP device 104. In some examples, user device 102 may cache the username and/or password such that the user need not enter the username and/or password. IDP device 106 sends a received username and password to authentication device 108, which determines whether the password is valid for the username, e.g., by comparing data for a received password associated with an account for the user to data for a stored password associated with the account. Authentication device 108 may hash data for the received and stored passwords using various hashing algorithms, such as salted hashes, in which a strong random number is used to salt the hash to provide hash randomization.

[0023] Authentication device 108 determines whether to authenticate a user based on comparing a password associated with a username in an authorization request to a password stored in association with the username in, for example, user credentials database 112. IDP device 106 receives user credentials (e.g., usernames and passwords) for user accounts from various devices, such as user device 102 via SP device 104. In response to receiving user credentials for a user account, IDP device 106 may initially submit the user credentials to authentication device 108 to determine whether the user credentials are authentic. Authentication device 108 may determine whether the user credentials are authentic, e.g., by identifying a stored password (or stored data representative of the password, such as a hashed password) in user credentials database 112. User credentials database 112 may include a table including usernames as key values and data representing passwords (e.g., hashed versions of passwords and salt values for the hashes) in rows corresponding to the key values. When the received password matches the expected password, authentication device 108 responds with a verification message. Conversely, when the received password

does not match the expected password, authentication device 108 responds with a failure message. Authentication device 108 may further be configured to lock a user account after a threshold number of password attempts have failed. In some examples, authentication device 108 includes a lockout counter for each user identifier. When authentication device 108 sends a failure message, it also increments the associated lockout counter. When the lockout counter satisfies (e.g., is greater than or equal to) a lockout threshold, authentication device 108 locks (e.g., prevents access to) the associated user account until an intervention clears the lockout. When authentication device 108 sends a verification message, it may reset the associated lockout counter.

[0024] Password failures may result from a variety of circumstances. For example, a user may have recently changed their password and the new password may not have propagated through the computer system yet (e.g., to authentication device 108, IDP device 106, and/or to a cache of a browser of user device 102 that automatically provides the user password on behalf of the user). Alternatively, the user may have recently changed their password and forgotten that the password had been changed and entered a previous password. Furthermore, the user account may be under attack by a malicious user attempting to gain illicit access to the user account, e.g., through a dictionary attack (which the lockout is designed to thwart).

[0025] In cases where a legitimate user has forgotten their password or is using a cached password of user device 102 that is not correct, lockout of the user's account may be said to be a false positive lockout, because the lockout is not actually thwarting a malicious user attack. This is as opposed to cases where a malicious user is in fact attempting to access the user's account and a lockout results. False positive lockouts tend to upset users, who must then either wait until a lockout period has expired, and possibly change passwords, potentially with the assistance of trusted administrators such as help desk administrators of an IDP system including IDP device 106 and/or authentication device 108. Accordingly, false positive lockouts can increase human user downtime while attempting to gain legitimate access to SP device 104, as well as increased network traffic and processing by and between user device 102, SP device 104, IDP device 106, and authentication device 108.

[0026] The techniques of this disclosure may reduce false positive lockouts. As a result of reducing false positive lockouts, the techniques of this disclosure may improve the performance of user device 102, SP device 104, IDP device 106, and authentication device 108, as well as reduce bandwidth consumed within network 100 for communications between these devices, due to resolving the false positive lockout. Furthermore, these techniques may improve experiences by both users and administrators. In this manner, these techniques may improve both computing devices and the field of network security, in particular, authentication and authorization.

[0027] The device operating the authentication service (e.g., IDP device 106) detects scenarios that are indicative of resulting in false positive lockouts. For ECP-based SAML authentication, for example, SP device 104 directly contacts IDP device 106 for authentication, i.e., to send ECP requests on behalf of user device 102. If the ECP request results in an authentication failure, SP device 104 may submit multiple ECP requests including the same user credentials, which may result in a false positive lockout. As another example, if a user of user device 102 changes a password on authentication device 108, but a device using ECP to access services of SP device 104 (e.g., user device 102, a gateway device, or other such device) is not updated with the new password, the ECP requests would be sent with the old password. In that case, the authentication device 108 would determine that authentication has failed, and IDP device 106 may be flooded with ECP requests continually. In such an example, since IDP device 106 sends all requests to authentication device 108, authentication device 108 would lock the user account when the configured threshold number of wrong password attempts has been exceeded.

[0028] IDP device 106, SP device 104, gateway devices, and/or user devices themselves may be configured to throttle authentication requests to prevent account lockout, while permitting authentication requests submitted as part of a brute force attack to be submitted to prompt the lockout. IDP device 106, SP device 104, and/or authentication device 108 may further be configured to generate reports representing, for example, numbers of accounts that have been locked out and/or a number of failed login attempts (excluding password duplications), e.g., to determine whether or not a brute force attack is being conducted against multiple user accounts. IDP device 106, SP device 104, and/or authentication device 108 may further generate an alert to be sent to an administrator to warn of such an ongoing brute force attack, e.g., if a number of account lockouts over a configured period of time exceeds a threshold.

[0029] If the authentication service receives multiple authentication requests with the same password, the authentication service avoids submitting authentication requests with repeated passwords to authentication device 108. Thus, authentication device 108 would not receive multiple authentication requests including the same password, thereby preventing lockout by preventing incrementing of a lockout counter associated with the user account. Accordingly, brute force attacks (also referred to as dictionary attacks) would still cause lockout.

[0030] IDP device 106 determines that the submitted password is not valid for the user account in response to receiving the failure message from authentication device 108. IDP device 106 stores the user credentials (e.g., username and password, or a salted hashed version thereof, along with the salt value) in attempt table 110. Subsequently, if IDP device 106 receives an authentication request associated with the username, IDP device

106 compares the password (e.g., or a hash thereof) in the authentication request to the password stored in user attempt table 110. If the new password is the same as the password stored in attempt table 110, IDP device 106 does not forward the authentication request to authentication device 108. In this manner, IDP device 106 may prevent authentication device 108 from incrementing the lockout counter for repeated instances of the same invalid password, thereby avoiding false positive lockout of the user account.

[0031] In some examples, IDP device 106 stores a salted hashed version of a password. To salt the hash, IDP device 106 used a salt value, such as a strong random number, when the password was hashed, and also use the salt value as an input to a hash function applied to the password. In this manner, when IDP device 106 subsequently receives a new authentication request associated with the user account, IDP device 106 retrieves the previous salt value and apply the hash function using the salt value to the password in the new authentication request to construct a new salted hashed password. IDP device 106 compares the new salted hashed password to the stored salted hashed password in attempt table 110 to determine whether the newly received password is the same as the previously received password. In some examples, IDP device 106 stores data representing multiple invalid passwords for a given user account in attempt table 110, where the data for each of the invalid passwords may be salted and hashed. Thus, IDP device 106 may store individual salt values for each of the multiple invalid passwords. In such examples, the first time one of the invalid passwords is used, the corresponding authentication request is forwarded to authentication device 108. Thus, in some examples, IDP device 106 may store multiple invalid passwords up to the lockout threshold of authentication device 108.

[0032] Accordingly, in some examples, for each unique password received for a given user account, IDP device 106 stores a salted hashed version of the password in attempt table 110. IDP device 106 stores the salt values used to construct the salted hashed versions of the passwords. Thus, IDP device 106 applies the hash function and corresponding salt value for each stored password to each newly received password for a given user account to determine whether the newly received password is the same as any of the stored passwords for the user account. If the newly received password is the same as any of the stored passwords for the user account, IDP device 106 avoids submitting the newly received password to authentication device 108.

[0033] In some examples, the invalid passwords are stored in attempt table 110 temporarily. In some such examples, invalid password(s) for a user account is associated with a timer that begins when a failure message is received from authentication device 108. When the timer expires, IDP device 106 deletes the associated password(s). Thus, if the password is received in an authorization request after the timer, IDP device 106 for-

wards the authentication request. In some examples, the time limit of the timer is set to a duration that takes into account propagation time between changing a password authentication device 108 and having the change implemented. Alternatively or additionally, in some example, the time limit of the timer is set to a duration that provides an opportunity for the user to change the passwords stored on the endpoint devices 102. For example, the time limit of the timer may be thirty seconds, one minute, two minutes, etc.

[0034] IDP device 106 may prevent false positive lockouts by preventing the same password from being sent to authentication device 108. However, authentication device 108 can still successfully lock out accounts being subjected to a dictionary attack by a malicious user, because IDP device 106 will continue to submit new passwords to authentication device 108.

[0035] Although the techniques described above are attributed to IDP device 106 for purposes of example and explanation above, it should be understood that in other examples, other devices may perform these or similar techniques. For example, SP device 104 may also include a user credentials database (not shown in FIG. 1) and perform the techniques attributed to IDP device 106. Similarly, user device 102 may itself perform these or similar techniques.

[0036] Moreover, in some examples, authentication device 108 may implement techniques as described above and/or IDP device 106 may be incorporated into authentication device 108. That is, in some examples, authentication device 108 may store both actual valid passwords for a user account and failed attempted passwords in user credentials database 112. In such examples, authentication device 108 compare newly received passwords to the actual valid password to determine whether to authenticate the user account, and if the password is invalid, compare the newly received password to stored failed attempted passwords. When the newly received password is not valid and is not stored as a failed password, authentication device 108 increments the lockout counter. Otherwise, if the newly received password is a failed password that is stored in, for example, user credentials database 112, authentication device 108 does not increment of the lockout counter.

[0037] In some examples, one or more of the user device 102, SP device 104, and/or IDP device 106 includes a mechanism as described above to identify and stop duplicate passwords (e.g., ECP requests) from being sent to authentication device 108. That is, these devices cache data representative of attempted passwords for a user account when a series of authentication requests (e.g., ECP requests) fails for the same user over a time duration (e.g., a minute). These devices may associate the invalid (wrong) password with a time within which all authentication requests for the particular user using the same password will not be sent to authentication device 108.

[0038] In some examples, any of user device 102, SP

device 104, and/or IDP device 106 include a user interface (UI) option for enabling password throttling. A UI option is provided for resetting such accounts that are blocked. In some examples, these devices further maintain a blocked table including a username, a password hash, a time at which the user was blocked, a time of a last authentication (e.g., ECP) request, a duplicate request count for the password, an expiration time, a user agent, and a realm value. The username field may correspond to a user account from a request packet, such as an ECP request packet. The password hash may correspond to the wrong password that failed authentication by authentication device 108. The time at which the user was blocked may represent the start time of a lockout, and may be used to determine when the user's account will be unlocked. The time of the last authentication request may correspond to a timestamp value of an ECP request packet. The duplicate request count may represent a total number of times the same password was received, overall or since the user account was locked out. The expiration time may represent the time until a password entry becomes valid. Such data may be stored in, e.g., attempt table 110.

[0039] In some examples, there are multiple such entries for each user account, up to a determined maximum number of entries (e.g., five). In some such examples, the entries are replaced in a first-in-first-out order. In some examples, the expiration time varies based on a number of authentication attempts over a time duration (e.g., one minute). For example, each incorrect password attempt may increase the time duration with diminishing returns. Alternatively, in some examples, the expiration time is set to a predetermined time, such as a minute. Before expiry, if a user attempts another password request with a duplicate password, the expiration time may be increased.

[0040] User device 102, SP device 104, IDP device 106, and authentication device 108 may each include one or more respective processors implemented in circuitry. Such processors may include one or more microprocessors, digital signal processors (DSPs), field programmable gate arrays (FPGAs), application specific integrated circuits (ASICs), or the like, alone or in any combination. Various processors may execute software instructions stored in memory units implemented in circuitry of these devices. Thus, the techniques of this disclosure may be realized in hardware, software, firmware, or a combination thereof. When realized in software or firmware, requisite hardware (such as a memory to store instructions and a processor to execute the instructions) may also be provided.

[0041] In this manner, each of user device 102, SP device 104, IDP device 106, and authentication device 108 represents an example of a computing device comprising one or more processors implemented in circuitry and configured to, in response to determine that the first password is not valid, incrementing a lockout counter associated with the user account; determine that a received

second password for the user account is the same as the first password; and in response to determining that the second password is the same as the first password, prevent incrementing of the lockout counter.

[0042] Likewise, each of user device 102, SP device 104, and IDP device 106 represents an example of a computing device comprising one or more processors implemented in circuitry and configured to send a first password for a user account to an authentication device; determine that the authentication device indicated that the first password is not valid for the user account; determine that a received second password for the user account is the same as the first password; and in response to determining that the second password is the same as the first password, prevent sending of the second password to the authentication device.

[0043] The techniques of this disclosure may be used in a variety of use cases or scenarios. Various examples of such scenarios are described below, although the scenarios discussed below are merely examples and are not exhaustive.

[0044] FIG 2 illustrates a scenario in which a password on authentication device 108 is changed for a user account (and stored in user credentials database 112), then later, a password cached on user device 102 is changed. In this scenario, initially, client device 102 sends the old (cached) password (PW1) to IDP device 106 via SP device 104. This causes IDP device 106 to forward the password (PW1) to authentication device 108. Since this is the first attempt, the authentication attempt fails (e.g., authentication device 108 sends a failure message). IDP device 106 stores the invalid password in association with the username (e.g., or a hash thereof) in the attempt table 110. SP device 104 send another authentication request with the same password to IDP device 106. For example, SP device 104 may resend the authentication request because it did not receive a SAML assertion. Alternatively or additionally, for example, SP device 106 may send another authentication request in response to receiving another request from user device 102. Alternatively or additionally, for example, multiple user devices 102A and 102B may have cached the same, old password when a user has changed their password as stored in user credentials database 112 with authentication device 108 such that each user device 102A and 102B independently send authentication requests with the incorrect password in a relatively short period of time.

[0045] IDP device 106 checks the password (PW1) of the new authentication request against the password(s) stored on attempt table 110 for the user. Because the IDP device 106 determines the new password to be a duplicate of the password on attempt table 110, IDP device 106 discards the authentication request and logs the attempt in, e.g., attempt table 110. Subsequently, SP device 104 may continue to generate the same authentication requests, and IDP device 106 may continue to block these requests having the same password. The user may change the password (PW2) that that user device 102

uses to match the password (PW2) stored in credential database 112. Because the subsequent authentication request includes a new password, IDP device 106 submits the authentication request to authentication device 108. In this example, authentication device 108 determines that the request is valid, because the password matches the password stored in user credentials database 112.

[0046] FIG. 3 illustrates a scenario in which a password on authentication device 108 is changed for a user account (and stored in user credentials database 112), then later, a password cached on user device 102 is changed. In this scenario, initially, client device 102 sends the old (cached) password (PW1) to IDP device 106 via SP device 104. This causes IDP device 106 to forward the password (PW1) to authentication device 108. Since this is the first attempt, the authentication attempt fails (e.g., authentication device 108 sends a failure message). IDP device 106 stores the invalid password (PW1) in association with the username (e.g., or a hash thereof) in the attempt table 110. SP device 104 send another authentication request with the same password to IDP device 106. For example, SP device 104 may resend the authentication request because it did not receive a SAML assertion. Alternatively, for example, SP device 106 may send another authentication request in response to receiving another request from user device 102. IDP device 106 checks the password (PW1) of the new authentication request against the password(s) stored on attempt table 110 for the user. Because the IDP device 106 determines the new password to be a duplicate of the password on attempt table 110, IDP device 106 discards the authentication request and logs the attempt in, e.g., attempt table 110. Subsequently, SP device 104 may continue to generate the same authentication requests, and IDP device 106 may continue to block these requests having the same password.

[0047] While the example of FIG. 3 illustrated one user device 102, multiple user devices 102A and 102B may have the same, old password after a user changes the password of authentication device 108 stored in user credentials database 112. The user may only change the cached password of one user device 102A. The other user device(s) 102B, using the old password, may cause an entry for the corresponding user in attempt table 110. When one of the user devices 102A changes to the new, correct password, the new password will not match the entry in attempt table 110. So, IDP device 106 will permit the new password to be sent to authentication device 108, and the submitting client device will be granted access. Other authentication requests for the user that send the old password will be blocked until the cached passwords are changed.

[0048] In the illustrated example, the user may mistakenly change the password that that user device 102 uses to a different incorrect password (PW2). For example, the user may submit a different, incorrect password after noticing that the first password (PW1) was not valid. Be-

cause the subsequent authentication request includes a new password, IDP device 106 submits the authentication request to authentication device 108. This causes IDP device 106 to forward the password (PW2) to authentication device 108. Since the second password (PW2) is also incorrect, the authentication attempt fails (e.g., authentication device 108 sends a failure message). IDP device 106 stores the invalid password (PW2) in association with the username (e.g., or a hash thereof) in the attempt table 110. SP device 104 send another authentication request with the same password to IDP device 106. For example, SP device 104 may resend the authentication request because it did not receive a SAML assertion. Alternatively, for example, SP device 106 may send another authentication request in response to receiving another request from user device 102. IDP device 106 checks the password (PW2) of the new authentication request against the passwords (PW1 and PW2) stored on attempt table 110 for the user. Because the IDP device 106 determines the new password to be a duplicate of one of the passwords on attempt table 110, IDP device 106 discards the authentication request and logs the attempt in, e.g., attempt table 110. Subsequently, SP device 104 may continue to generate the same authentication requests, and IDP device 106 may continue to block these requests having the same password. The user may then change the password stored by user device 102 to be the correct password (PW3). In this example, authentication device 108 determines that the request is valid, because the password matches the password stored in user credentials database 112.

[0049] FIG. 4 illustrates a scenario in which authentication device 108 updates a password for a user account relatively slowly and the user updates passwords on user devices 102A and 102B before the password has actually changed on authentication device 108 (e.g., in user credentials database 112). In the illustrated example, the password is change on user device 102A. User device 102A sends an authentication request with the new password (PW2). This causes IDP device 106 to forward the password (PW2) to authentication device 108. Because the new password (PW2) has not been updated in credentials database 112, the authentication attempt fails (e.g., authentication device 108 sends a failure message). IDP device 106 stores the allegedly invalid password in association with the username (e.g., or a hash thereof) in the attempt table 110. Additionally, in the illustrated example, IDP device 106 starts a timer associated with the incorrect password (PW2). Subsequently, the password stored by user device 102B is updated to the new password (PW2). User device 102B sends an authentication request with the new password (PW2). The SP device 106 forwards the authentication request. Because the new password (PW2) matches the old password in the attempt table 110, IDP device 106 does not forward the authentication request to authentication device 108. This may continue until the password in credentials database 112 updates to reflect the new pass-

word (PW2) and the time expires causing IDP 106 to delete the new password (PW2) from attempt table 110. Subsequently, when user device 102B sends an authentication request with the new password (PW2), authentication device 108 will authorize access.

[0050] FIG. 5 illustrates a scenario in which a brute force attack is perpetrated by a malicious actor. In this case, for the same username, IDP device 106 will receive multiple different passwords. So, for that user, IDP device 106 stacks each of the different passwords in entries of attempt table 110, and submits each of the different passwords to authentication device 108. In some cases, IDP device 106 may temporarily block attempts, e.g., allowing only up to five attempts per minute. In the illustrated example, IDP device 106 stores the various password attempts on attempt table 110. However, in a brute force attack, passwords are not generally repeated. Thus, IDP device 106 does not block any of the password attempts that include unique passwords. Accordingly, authentication device 108 may ultimately lockout the user account to which the attack is directed.

[0051] FIG. 6 is a flowchart illustrating an example method for performing techniques of this disclosure. For purposes of example, the method of FIG. 6 is explained with respect to IDP device 106 of FIG. 1. However, it should be understood that the method of FIG. 6 may be performed by other devices, such as user device 102, SP device 104, or authentication device 108 of FIG. 1, or another device involved in authenticating user credentials including a password.

[0052] Initially, in this example, IDP device 106 receives a first password for a user account (600). IDP device 106 determines that the first password is not valid for the user (602). For example, IDP device 106 may send the password, along with a username, to authentication device 108, and authentication device 108 may send data back to IDP device 106 indicating that the password is invalid. In other examples, IDP device 106 itself (or another device performing the method) may have access to data representative of the valid password to itself determine whether the password is valid.

[0053] IDP device 106 then stores data for the password (604), such as a salted hashed version of the password and a salt value used to generate the salted hashed version. IDP device 106 stores this data in attempt table 110. In the illustrated example, IDP device 106 also increments a lockout counter (606). The lockout counter may be maintained by IDP device 106 itself, or by a separate device, such as authentication device 108. Submitting an invalid password to authentication device 108 may cause authentication device 108 to increment a lockout counter maintained by authentication device 108.

[0054] IDP device 106 (or authentication device 108) determines whether the lockout counter is greater than a threshold value (608). If the lockout counter exceeds the threshold value ("YES" branch of 608), IDP device 106 or authentication device 108 performs a lockout on the user account (610). However, if the lockout counter

does not exceed (i.e., is less than or equal to) the threshold ("NO" branch of 608), IDP device 106 waits for a subsequent authentication attempt.

[0055] After receiving a new password for the same user account (612), IDP device 106 determines whether the new password is different than one or more previous passwords attempted for the user account (614). For example, IDP device 106 may hash the new password with salt values associated with the previous passwords to generate salted hashed versions of the new password, and compare each of the salted hashed versions of the new password with the stored salted hashed passwords stored in attempt table 110. If the new password is not different than (i.e., is the same as) at least one of the previous passwords ("NO" branch of 614), IDP device 106 avoids incrementing the lockout counter (e.g., directly, or by preventing sending of the new password to authentication device 108) and again awaits a new password.

[0056] However, if the new password is different than each of the previous passwords ("YES" branch of 614), IDP device 106 may determine whether the password is valid (616). For example, IDP device 106 may send the password to authentication device 108. If the new password is not valid ("NO" branch of 616), IDP device 106 may store a salted hashed version of the new password (604) and authentication device 108 may increment the lockout counter (606). However, if the new password is valid ("YES" branch of 616), IDP device 106 may grant access to serves to the user (618). For example, IDP device 106 may indicate one or more services that SP device 104 may provide to the user.

[0057] In this manner, the method of FIG. 6 represents an example of a method including determining that a received first password for a user account is not valid for the user account; in response to determining that the first password is not valid, incrementing a lockout counter associated with the user account; determining that a received second password for the user account is the same as the first password; and in response to determining that the second password is the same as the first password, preventing incrementing of the lockout counter.

[0058] The method of FIG. 6 also represents an example of a method including sending a first password for a user account to an authentication device; determining that the authentication device indicated that the first password is not valid for the user account; determining that a received second password for the user account is the same as the first password; and in response to determining that the second password is the same as the first password, preventing sending of the second password to the authentication device.

[0059] FIG. 7 is a flowchart illustrating an example of a method for performing techniques of this disclosure. For purposes of example, the method of FIG. 7 is explained with respect to IDP device 106 of FIG. 1. However, it should be understood that the method of FIG. 7 may be performed by other devices, such as user device

102 or SP device 104 of FIG. 1, or another device involved in authenticating user credentials including a password.

[0060] In the example of FIG. 7, IDP device 106 initially receives a first password for a user account (702). IDP device 106 sends the password to authentication device 108 (704). IDP device 106 then determines whether the password is valid (706), e.g., based on a response from authentication device 108. When the response indicates that the password is valid ("YES" branch of 706), IDP device 106 grants the user access (708).

[0061] Otherwise, when the response indicates that the password is not valid ("NO" branch of 706), IDP device 106 stores data for the first password (710), e.g., in attempt table 110. As disclosed above, such data may include a salted hashed version of the password, as well as a salt value used to generate the salted hashed version. IDP device 106 subsequently receives a new password for the user account (712). IDP device 106 determines whether the new password is different than one or more previous passwords attempted for the user account (714). For example, IDP device 106 may hash the new password with salt values associated with the previous passwords to generate salted hashed versions of the new password, and compare each of the salted hashed versions of the new password with the stored salted hashed passwords stored in attempt table 110. When the new password is not different than (i.e., is the same as) at least one of the previous passwords ("NO" branch of 714), IDP device 106 does not send the password to authentication device 108. However, when the new password is different than the previous passwords for the user account ("YES" branch of 714), IDP device 106 sends the password to authentication device 108 (704). In some examples, authentication device 108 performs a lockout of the user account if too many invalid password attempts are made.

[0062] In this manner, the method of FIG. 7 represents an example of a method including sending a first password for a user account to an authentication device; determining that the authentication device indicated that the first password is not valid for the user account; determining that a received second password for the user account is the same as the first password; and in response to determining that the second password is the same as the first password, preventing sending of the second password to the authentication device.

[0063] Although generally described with respect to preventing false positive lockouts of individual user accounts in response to duplicated password attempts, the techniques of this disclosure may be used to prevent false positive lockouts in other scenarios as well. For example, some systems lock out source IP addresses, ranges of source IP addresses, geographic locations inferred from IP addresses, or other elements such as HTTP attributes "X-Forwarded-For" or "User Agent." The techniques of this disclosure may be used to prevent false positive lockouts in any of these scenarios as well.

[0064] The techniques described in this disclosure

may be implemented, at least in part, in hardware, software, firmware or any combination thereof. For example, various aspects of the described techniques may be implemented within one or more processors, including one or more microprocessors, digital signal processors (DSPs), application specific integrated circuits (ASICs), field programmable gate arrays (FPGAs), or any other equivalent integrated or discrete logic circuitry, as well as any combinations of such components. The terms "processor" or "processing circuitry" may generally refer to any of the foregoing logic circuitry, alone or in combination with other logic circuitry, or any other equivalent circuitry. A control unit comprising hardware may also perform one or more of the techniques of this disclosure.

[0065] Such hardware, software, and firmware may be implemented within the same device or within separate devices to support the various operations and functions described in this disclosure. In addition, any of the described units, modules or components may be implemented together or separately as discrete but interoperable logic devices. Depiction of different features as modules or units is intended to highlight different functional aspects and does not necessarily imply that such modules or units must be realized by separate hardware or software components. Rather, functionality associated with one or more modules or units may be performed by separate hardware or software components, or integrated within common or separate hardware or software components.

[0066] The techniques described in this disclosure may also be embodied or encoded in a computer-readable medium, such as a computer-readable storage medium, containing instructions. Instructions embedded or encoded in a computer-readable medium may cause a programmable processor, or other processor, to perform the method, e.g., when the instructions are executed. Computer-readable media may include non-transitory computer-readable storage media and transient communication media. Computer readable storage media, which is tangible and non-transitory, may include random access memory (RAM), read only memory (ROM), programmable read only memory (PROM), erasable programmable read only memory (EPROM), electronically erasable programmable read only memory (EEPROM), flash memory, a hard disk, a CD-ROM, a floppy disk, a cassette, magnetic media, optical media, or other computer-readable storage media. It should be understood that the term "computer-readable storage media" refers to physical storage media, and not signals, carrier waves, or other transient media.

[0067] Additionally, or alternatively, the techniques discussed herein may be realized at least in part by a computer readable communication medium that carries or communicates code in the form of instructions or data structures and that can be accessed, read, and/or executed by a computer. In other words, any suitable computer readable medium may be used, which comprises instructions and which can for example be a transitory

medium, such as a communication medium, or a non-transitory medium, such as a storage medium.

[0068] From one perspective, there has now been described a server to provide single sign on services. The server includes a processor and a memory storing an attempt table. The server, in response to receiving a first password for a user account, forwards the first password to an authentication device. The server determines that the first password is not valid for the user account. The server stores the first password in association with the user account in the attempt table. In response to receiving a second password for the user account, the server determines whether the second password matches the first password. When the second password does not match the first password, the server forwards the second password to the authentication device.

[0069] Various examples have been described. These and other examples may be within the scope of the invention which is defined in the following claims.

Claims

1. A method of operating a server (106) to provide a single sign on service for multiple service providers, the server comprising a memory storing an attempt table (110), the method comprising:

in response to receiving (702) a first password for a user account, forwarding (704) the first password to an authentication device (108);
determining that the first password is not valid for the user account;
storing (710) data representative of the first password in association with the user account in the attempt table;
in response to receiving (712) a second password for the user account, determining (714) whether the second password matches the first password; and
when the second password does not match the first password, forwarding (704) the second password to the authentication device.

2. The method of claim 1, further comprising:

in response to determining that a received third password for the user account is different than the first password, forwarding the third password to the authentication device;
determining that the third password is not valid for the user account;
in response to determining that the third password is not valid, storing data representative of the third password in association with the user account in the attempt table;
determining that a received fourth password for the user account is the same as one of the first

password or the third password; and
in response to determining that the fourth password is the same as the first password or the third password, not forwarding the fourth password to the authentication device.

3. The method of claim 2, further comprising:

performing a first salted hash on the first password to generate a first salted hashed password, wherein storing data representative of the first password comprises storing in the attempt table the first salted hashed password and a first salt value for the first salted hashed password; and
performing a second salted hash on the third password to generate a second salted hashed password, wherein storing data representative of the third password comprises storing in the attempt table the second salted hashed password and a second salt value for the second salted hashed password;
wherein determining that the fourth password is the same as one of the first password or the third password comprises:

performing a third salted hash on the fourth password using the first salt value to generate a third salted hashed password;
performing a fourth salted hash on the fourth password using the second salt value to generate a fourth salted hashed password;
and
determining that one of the third salted hashed password is the same as the first salted hashed password or the fourth salted hashed password is the same as the second salted hashed password.

4. The method of any one of claims 1 to 3, wherein determining that the first password is not valid comprises:
receiving, from the authentication device, data indicating that the first password is not valid.

5. A server (106) operating to provide a single sign on service for multiple service providers, the server comprising:

a memory storing an attempt table (110); and
a processor implemented in circuitry and configured to:

in response to receiving (702) a first password for a user account, forward (704) the first password to an authentication device;
determine that the first password is not valid for the user account;
store (710) data representative of the first

- password in association with the user account in the attempt table;
 in response to receiving (712) a second password for the user account, determine (714) whether the second password matches the first password; and
 when the second password does not match the first password, forward (704) the second password to the authentication device. 5
6. The server of claim 5, wherein the processor of the server is further configured to:
- in response to storing the first password in association with the user account in the attempt table, start a timer;
 when the timer expires, delete the first password from the attempt table. 15
7. The server of claim 6, wherein the processor of the server is further configured to, in response to receiving, after the timer has expired, a third password for the user account that matches the first password, forward the third password to an authentication device. 20
8. The server of any one of claims 5 to 7, wherein the first password originates from a first user device and the second password originates from a second user device. 25
9. The server of any one of claims 5 to 7, wherein to store the first password in association with the user account in the attempt table further comprises, the processor of the server is further configured to: 30
- generate a first hash of the first password with a first salt value; and
 store the first hash and the first salt value in association with the user account in the attempt table. 35
10. The server of claim 9, wherein to determine whether the second password matches the first password, the processor of the server is further configured to: 40
- generate a second hash of the second password with the first salt value; and
 determine that the second password matches the first password when the second hash matches the first hash. 45
11. The server of any one of claims 5 to 10, wherein the processor of the server is further configured to: 50
- in response to receiving a third password for the user account, determine whether the third password matches the first password;
- when the third password does not match the first password, forward the third password to the authentication device;
 determine that the third password is not valid for the user account; and
 store the third password in association with the user account in the attempt table.
12. The server of claim 11, wherein the processor of the server is further configured to:
- in response to receiving a fourth password for the user account, determine whether the fourth password matches either the first password or the third password;
 when the fourth password does not match either one of the first password or the third password, forward the fourth password to the authentication device.
13. A computer readable medium comprising instructions that, when executed, cause a server (106) to:
- in response to receiving (702) a first password for a user account, forward (704) the first password to an authentication device (108);
 determine that the first password is not valid for the user account;
 store (710) the first password in association with the user account in an attempt table (110);
 in response to receiving (712) a second password for the user account, determine (714) whether the second password matches the first password; and
 when the second password does not match the first password, forward (704) the second password to the authentication device.
14. The computer readable medium of claim 13, wherein the instructions further cause the server to:
- in response to storing the first password in association with the user account in the attempt table, start a timer;
 when the timer expires, delete the first password from the attempt table.

Patentansprüche

1. Ein Verfahren für den Betrieb eines Servers (106), womit ein Single-Sign-On-Dienst für mehrere Service-Provider angeboten wird und der Server einen Speicher umfasst, in dem eine Zugriffsversuchstabelle (110) gespeichert ist; dabei weist das Verfahren folgende Schritte auf:

Als Reaktion auf den Eingang (702) eines ersten

- Passworts für ein Benutzerkonto wird das erste Passwort an ein Authentifizierungsgerät (108) weitergeleitet (704);
es wird festgestellt, dass das erste Passwort für das Benutzerkonto nicht gültig ist;
Daten, die für das erste Passwort in Verbindung mit dem Benutzerkonto repräsentativ sind, werden in der Zugriffsversuchstabelle gespeichert (710);
als Reaktion auf den Eingang (712) eines zweiten Passworts für das Benutzerkonto wird festgestellt (714), ob das zweite Passwort mit dem ersten Passwort übereinstimmt; und
wenn das zweite Passwort nicht mit dem ersten Passwort übereinstimmt, wird das zweite Passwort zum Authentifizierungsgerät weitergeleitet (704).
2. Das Verfahren nach Anspruch 1, das außerdem folgende Schritte umfasst:
- Als Reaktion auf die Feststellung, dass ein eingegangenes drittes Passwort für das Benutzerkonto vom ersten Passwort abweicht, wird das dritte Passwort an das Authentifizierungsgerät weitergeleitet;
es wird festgestellt, dass das dritte Passwort für das Benutzerkonto nicht gültig ist;
als Reaktion auf die Feststellung, dass das dritte Passwort ungültig ist, werden Daten, die repräsentativ für das dritte Passwort in Verbindung mit dem Benutzerkonto sind, in der Zugriffsversuchstabelle gespeichert;
es wird festgestellt, dass ein eingegangenes viertes Passwort für das Benutzerkonto mit dem ersten Passwort oder dem dritten Passwort übereinstimmt; und
als Reaktion auf die Feststellung, dass das vierte Passwort mit dem ersten Passwort oder dem dritten Passwort übereinstimmt, wird das vierte Passwort nicht an das Authentifizierungsgerät weitergeleitet.
3. Das Verfahren nach Anspruch 2, das außerdem folgende Schritte umfasst:
- Es wird eine erste Salted-Hash-Verschlüsselung des ersten Passworts durchgeführt und damit ein erstes Salted-Hash-Passwort generiert, wobei die Speicherung von Daten, die für das erste Passwort repräsentativ sind, die Speicherung des ersten Salted-Hash-Passworts und eines ersten Salt-Werts für das erste Salted-Hash-Passwort in der Zugriffsversuchstabelle umfasst; und
es wird eine zweite Salted-Hash-Verschlüsselung des dritten Passworts durchgeführt und damit ein zweites Salted-Hash-Passwort gene-
- riert, wobei die Speicherung von Daten, die für das dritte Passwort repräsentativ sind, die Speicherung des zweiten Salted-Hash-Passworts und eines zweiten Salt-Werts für das zweite Salted-Hash-Passwort in der Zugriffsversuchstabelle umfasst;
wobei die Feststellung, dass das vierte Passwort mit dem ersten Passwort oder dem dritten Passwort übereinstimmt, folgende Schritte umfasst:
- Es wird eine dritte Salted-Hash-Verschlüsselung des vierten Passworts durchgeführt und dabei der erste Salt-Wert zur Generierung eines dritten Salted-Hash-Passworts verwendet;
es wird eine vierte Salted-Hash-Verschlüsselung des vierten Passworts durchgeführt und dabei der zweite Salt-Wert zur Generierung eines vierten Salted-Hash-Passworts verwendet; und
es wird festgestellt, dass das dritte Salted-Hash-Passwort mit dem ersten Salted-Hash-Passwort oder das vierte Salted-Hash-Passwort mit dem zweiten Salted-Hash-Passwort übereinstimmt.
4. Das Verfahren nach einem der Ansprüche 1 bis 3, wobei die Feststellung, dass das erste Passwort ungültig ist, folgende Schritte umfasst:
Es werden Daten des Authentifizierungsgeräts empfangen, die anzeigen, dass das erste Passwort ungültig ist.
5. Ein Server (106) für den Betrieb eines Single-Sign-On-Dienstes für mehrere Service-Provider, wobei der Server aufweist:
- einen Speicher für die Speicherung einer Zugriffsversuchstabelle (110); und
einen Prozessor, der in Schaltkreisen aufgebaut ist und so konfiguriert ist, dass er:
- als Reaktion auf den Eingang (702) eines ersten Passworts für ein Benutzerkonto das erste Passwort an ein Authentifizierungsgerät übermittelt (704);
feststellt, dass das erste Passwort für das Benutzerkonto nicht gültig ist;
Daten, die repräsentativ für das erste Passwort in Verbindung mit dem Benutzerkonto sind, in der Zugriffsversuchstabelle speichert (710);
als Reaktion auf den Eingang (712) eines zweiten Passworts für das Benutzerkonto feststellt (714), ob das zweite Passwort mit dem ersten Passwort übereinstimmt; und
wenn das zweite Passwort nicht mit dem

- ersten Passwort übereinstimmt, das zweite Passwort an das Authentifizierungsgerät übermittelt (704).
6. Der Server nach Anspruch 5, wobei der Prozessor des Servers außerdem so konfiguriert ist, dass er:
- als Reaktion auf die Speicherung des ersten Passworts in Verbindung mit dem Benutzerkonto in der Zugriffsversuchstabelle einen Zeitgeber in Gang setzt;
wenn der Zeitgeber abgelaufen ist, das erste Passwort aus der Zugriffsversuchstabelle löscht.
7. Der Server nach Anspruch 6, wobei der Prozessor des Servers außerdem so konfiguriert ist, dass er als Reaktion darauf, dass er nach Ablauf des Zeitgebers ein drittes Passwort für das Benutzerkonto erhalten hat, das mit dem ersten Passwort übereinstimmt, das dritte Passwort an ein Authentifizierungsgerät übermittelt.
8. Der Server nach einem der Ansprüche 5 bis 7, wobei das erste Passwort aus einem ersten Benutzergerät stammt und das zweite Passwort aus einem zweiten Benutzergerät stammt.
9. Der Server nach einem der Ansprüche 5 bis 7, wobei, um das erste Passwort in Verbindung mit dem Benutzerkonto in der Zugriffsversuchstabelle zu speichern, der Prozessor des Servers außerdem so konfiguriert ist, dass er:
- eine erste Hash-Verschlüsselung des ersten Passworts mit einem ersten Salt-Wert generiert;
und
den ersten Hash-Wert und den ersten Salt-Wert in Verbindung mit dem Benutzerkonto in der Zugriffsversuchstabelle speichert.
10. Der Server nach Anspruch 9, wobei zur Feststellung, ob das zweite Passwort mit dem ersten Passwort übereinstimmt, der Prozessor des Servers außerdem so konfiguriert ist, dass er:
- eine zweite Hash-Verschlüsselung des zweiten Passworts mit dem ersten Salt-Wert generiert;
und
feststellt, dass das zweite Passwort mit dem ersten Passwort übereinstimmt, wenn die zweite Hash-Verschlüsselung mit der ersten Hash-Verschlüsselung übereinstimmt.
11. Der Server nach einem der Ansprüche 5 bis 10, wobei der Prozessor des Servers außerdem so konfiguriert ist, dass er:
- als Reaktion auf den Eingang eines dritten Passworts für das Benutzerkonto feststellt, ob das dritte Passwort mit dem ersten Passwort übereinstimmt;
wenn das dritte Passwort nicht mit dem ersten Passwort übereinstimmt, das dritte Passwort an das Authentifizierungsgerät übermittelt;
feststellt, dass das dritte Passwort für das Benutzerkonto ungültig ist; und
das dritte Passwort in Verbindung mit dem Benutzerkonto in der Zugriffsversuchstabelle speichert.
12. Der Server nach Anspruch 11, wobei der Prozessor des Servers außerdem so konfiguriert ist, dass er:
- als Reaktion auf den Eingang eines vierten Passworts für das Benutzerkonto feststellt, ob das vierte Passwort entweder mit dem ersten Passwort oder mit dem dritten Passwort übereinstimmt;
wenn das vierte Passwort mit dem ersten Passwort oder mit dem dritten Passwort nicht übereinstimmt, das vierte Passwort an das Authentifizierungsgerät übermittelt.
13. Ein computerlesbares Medium, welches Anweisungen enthält, die bei ihrer Ausführung bewirken, dass ein Server (106):
- als Reaktion auf den Eingang (702) eines ersten Passworts für ein Benutzerkonto das erste Passwort an ein Authentifizierungsgerät (108) übermittelt (704);
feststellt, dass das erste Passwort für das Benutzerkonto ungültig ist;
das erste Passwort in Verbindung mit dem Benutzerkonto in einer Zugriffsversuchstabelle (110) speichert (710);
als Reaktion auf den Eingang (712) eines zweiten Passworts für das Benutzerkonto feststellt (714), ob das zweite Passwort mit dem ersten Passwort übereinstimmt; und
wenn das zweite Passwort nicht mit dem ersten Passwort übereinstimmt, das zweite Passwort an das Authentifizierungsgerät übermittelt (704).
14. Das computerlesbare Medium nach Anspruch 13, wobei die Anweisungen außerdem bewirken, dass der Server:
- als Reaktion auf die Speicherung des ersten Passworts in Verbindung mit dem Benutzerkonto in der Zugriffsversuchstabelle einen Zeitgeber in Gang setzt;
wenn der Zeitgeber abgelaufen ist, das erste Passwort aus der Zugriffsversuchstabelle

löscht.

Revendications

1. Procédé d'opération d'un serveur (106) destiné à fournir un service à authentification unique pour de multiples fournisseurs de service, le serveur comprenant une mémoire stockant une table de tentatives (110), le procédé comprenant :
 - en réponse à la réception (702) d'un premier mot de passe d'un compte utilisateur, la transmission (704) du premier mot de passe à un dispositif d'authentification (108) ;
 - le fait d'établir que le premier mot de passe n'est pas valable pour le compte utilisateur ;
 - le stockage (710) de données représentatives du premier mot de passe en association avec le compte utilisateur dans une table de tentatives ;
 - en réponse à la réception (712) d'un deuxième mot de passe pour le compte utilisateur, le fait d'établir (714) si le deuxième mot de passe est égal au premier mot de passe ; et
 - lorsque le deuxième mot de passe n'est pas égal au premier mot de passe, la transmission (704) du deuxième mot de passe au dispositif d'authentification.
2. Procédé selon la revendication 1, comprenant en outre :
 - en réponse à l'établissement qu'un troisième mot de passe reçu pour le compte utilisateur est différent du premier mot de passe, la transmission du troisième mot de passe au dispositif d'authentification ;
 - le fait d'établir que le troisième mot de passe n'est pas valable pour le compte utilisateur ;
 - en réponse à l'établissement que le troisième mot de passe n'est pas valable, le stockage de données représentatives du troisième mot de passe en association avec le compte utilisateur dans la table de tentatives ;
 - le fait d'établir qu'un quatrième mot de passe reçu pour le compte utilisateur est identique à l'un parmi le premier mot de passe ou le troisième mot de passe ; et
 - en réponse à l'établissement que le quatrième mot de passe est identique au premier mot de passe ou au troisième mot de passe, la non-transmission du quatrième mot de passe au dispositif d'authentification.
3. Procédé selon la revendication 2, comprenant en outre :
 - l'application d'un premier hachage salé au pre-
- mier mot de passe afin de générer un premier mot de passe haché et salé, selon lequel le stockage de données représentatives du premier mot de passe comprend le stockage dans la table de tentatives du premier mot de passe haché et d'une première valeur de salage pour le premier mot de passe haché et salé ; et
- l'application d'un deuxième hachage salé au troisième mot de passe afin de générer un deuxième mot de passe haché et salé, selon lequel le stockage de données représentatives du troisième mot de passe comprend le stockage dans la table de tentatives du deuxième mot de passe haché et d'une deuxième valeur de salage pour le deuxième mot de passe haché et salé ;
- selon lequel le fait d'établir que le quatrième mot de passe est identique à l'un parmi le premier mot de passe ou le troisième mot de passe comprend :
 - l'application d'un troisième hachage salé au quatrième mot de passe en utilisant la première valeur de salage afin de générer un troisième mot de passe haché et salé ;
 - l'application d'un quatrième hachage salé au quatrième mot de passe en utilisant la deuxième valeur de hachage afin de générer un quatrième mot de passe haché et salé ; et
 - le fait d'établir que soit le troisième mot de passe haché et salé est identique au premier mot de passe haché et salé, soit le quatrième mot de passe haché et salé est identique au deuxième mot de passe haché et salé.
4. Procédé selon l'une quelconque des revendications 1 à 3, selon lequel le fait d'établir que le premier mot de passe n'est pas valable comprend :
 - la réception, en provenance du dispositif d'authentification, de données indiquant que le premier mot de passe n'est pas valable.
5. Serveur (106) opérant pour fournir un service à authentification unique pour de multiples fournisseurs de service, le serveur comprenant :
 - une mémoire stockant une table de tentatives (110) ; et
 - un processeur implémenté en circuits et configuré pour :
 - en réponse à la réception (702) d'un premier mot de passe d'un compte utilisateur, transmettre (704) le premier mot de passe à un dispositif d'authentification ;
 - établir que le premier mot de passe n'est

- pas valable pour le compte utilisateur ;
stocker (710) des données représentatives du premier mot de passe en association avec le compte utilisateur dans la table de tentatives ;
en réponse à la réception (712) d'un deuxième mot de passe pour le compte utilisateur, établir (714) si le deuxième mot de passe est égal au premier mot de passe ; et
lorsque le deuxième mot de passe n'est pas égal au premier mot de passe, transmettre (704) le deuxième mot de passe au dispositif d'authentification.
6. Serveur selon la revendication 5, selon lequel le processeur du serveur est en outre configuré pour :
- en réponse au stockage du premier mot de passe en association avec le compte utilisateur dans la table de tentatives, faire démarrer un minuteur ;
lorsque le minuteur expire, supprimer le premier mot de passe de la table de tentatives.
7. Serveur selon la revendication 6, selon lequel le processeur du serveur est en outre configuré pour, en réponse à la réception, après expiration du minuteur, d'un troisième mot de passe pour le compte utilisateur qui est identique au premier mot de passe, transmettre le troisième mot de passe à un dispositif d'authentification.
8. Serveur selon l'une quelconque des revendications 5 à 7, selon lequel le premier mot de passe provient d'un premier dispositif utilisateur et le deuxième mot de passe provient d'un deuxième dispositif utilisateur.
9. Serveur selon l'une quelconque des revendications 5 à 7, selon lequel afin de stocker le premier mot de passe en association avec le compte utilisateur dans la table de tentatives, le processeur du serveur est en outre configuré pour :
- générer un premier hachage du premier mot de passe avec une première valeur de salage ; et
stocker le premier hachage et la première valeur de salage en association avec le compte utilisateur dans la table de tentatives.
10. Serveur selon la revendication 9, selon lequel afin d'établir si le deuxième mot de passe est identique au premier mot de passe, le processeur du serveur est en outre configuré pour :
- générer un deuxième hachage du deuxième mot de passe avec la première valeur de salage ; et
- établir que le deuxième mot de passe est identique au premier mot de passe lorsque le deuxième hachage est identique au premier hachage.
11. Serveur selon l'une quelconque des revendications 5 à 10, selon lequel le processeur du serveur est en outre configuré pour :
- en réponse à la réception d'un troisième mot de passe pour le compte utilisateur, établir si le troisième mot de passe est identique au premier mot de passe ;
lorsque le troisième mot de passe n'est pas identique au premier mot de passe, transmettre le troisième mot de passe au dispositif d'authentification ;
établir que le troisième mot de passe n'est pas valable pour le compte utilisateur ; et
stocker le troisième mot de passe en association avec le compte utilisateur dans la table de tentatives.
12. Serveur selon la revendication 11, selon lequel le processeur du serveur est en outre configuré pour :
- en réponse à la réception d'un quatrième mot de passe pour le compte utilisateur, établir si le quatrième mot de passe est identique soit au premier mot de passe, soit au troisième mot de passe ;
lorsque le quatrième mot de passe n'est pas identique à l'un des premier ou troisième mots de passe, transmettre le quatrième mot de passe au dispositif d'authentification.
13. Moyen lisible par ordinateur comprenant des instructions qui, lorsqu'elles sont exécutées, ont pour effet de faire fonctionner un serveur (106) de manière à :
- en réponse à la réception (702) d'un premier mot de passe d'un compte utilisateur, transmettre (704) le premier mot de passe à un dispositif d'authentification (108) ;
établir que le premier mot de passe n'est pas valable pour le compte utilisateur ;
stocker (710) le premier mot de passe en association avec le compte utilisateur dans une table de tentatives (110) ;
en réponse à la réception (712) d'un deuxième mot de passe pour le compte utilisateur, établir (714) si le deuxième mot de passe est égal au premier mot de passe ; et
lorsque le deuxième mot de passe n'est pas égal au premier mot de passe, transmettre (704) le deuxième mot de passe au dispositif d'authentification.
14. Moyen lisible par ordinateur selon la revendication

13, selon lequel les instructions ont en outre pour effet de faire fonctionner le serveur de manière à :

en réponse au stockage du premier mot de passe en association avec le compte utilisateur dans la table de tentatives, faire démarrer un minuteur ;
lorsque le minuteur expire, supprimer le premier mot de passe de la table de tentatives.

5
10

15

20

25

30

35

40

45

50

55

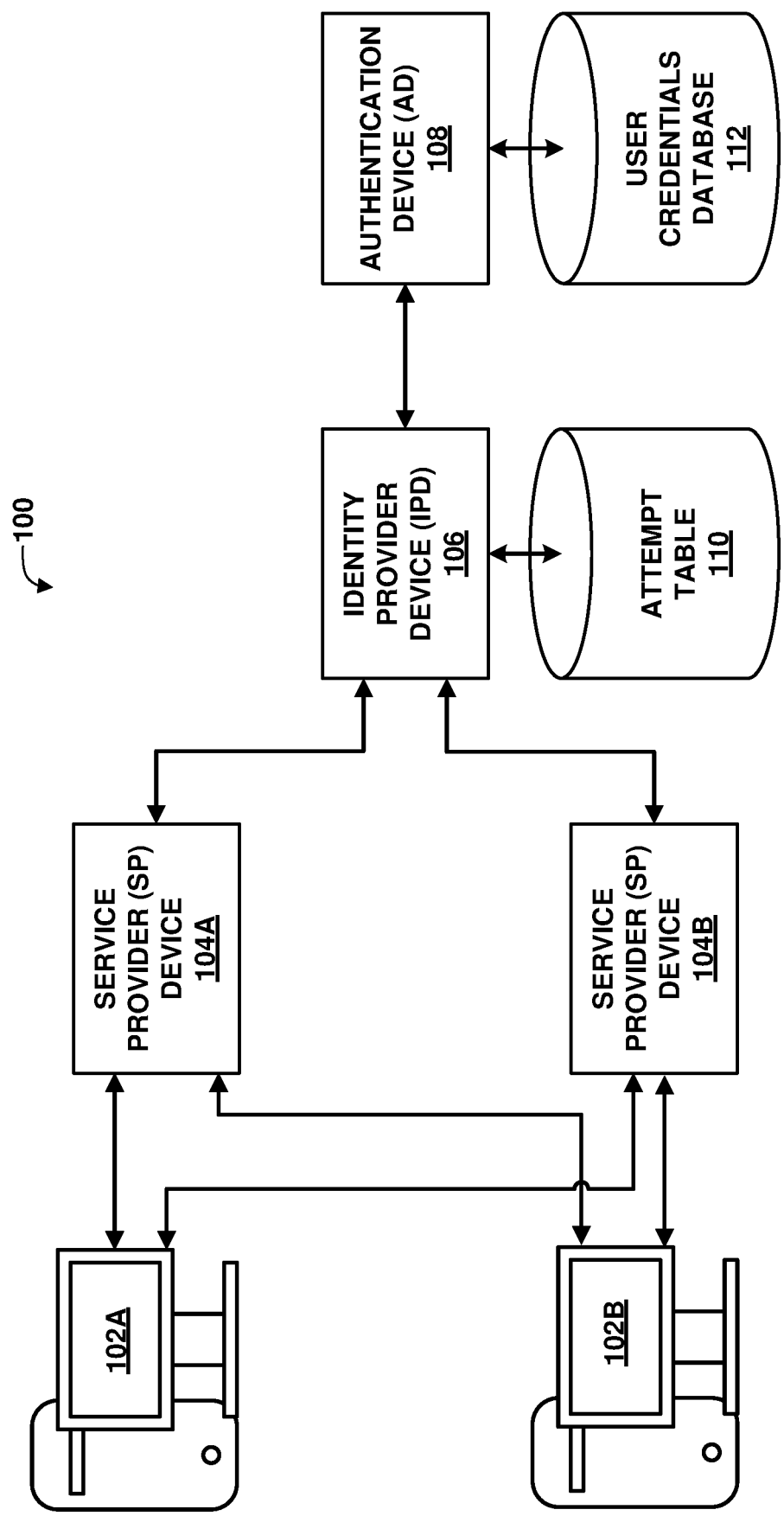


FIG. 1

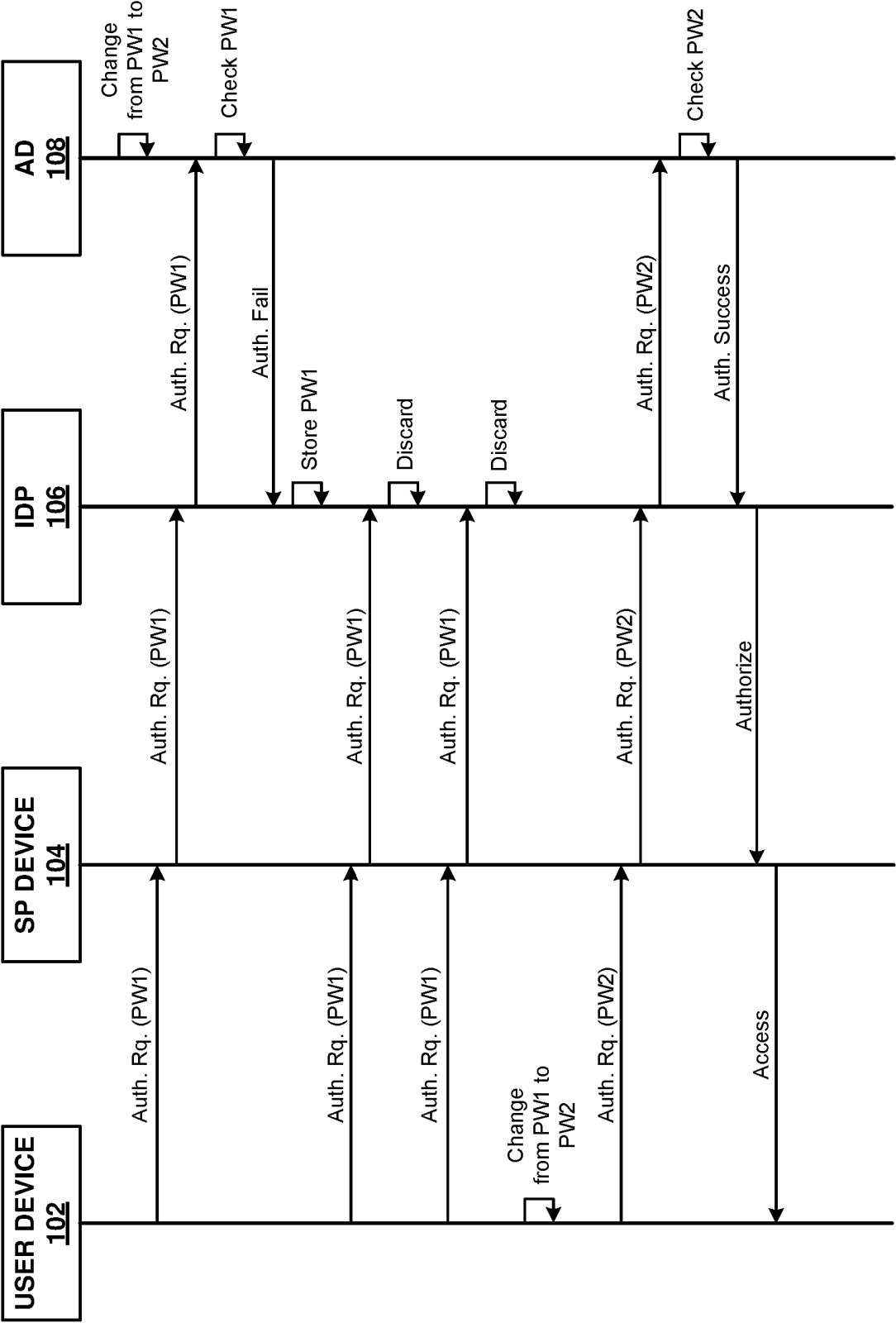


FIG. 2

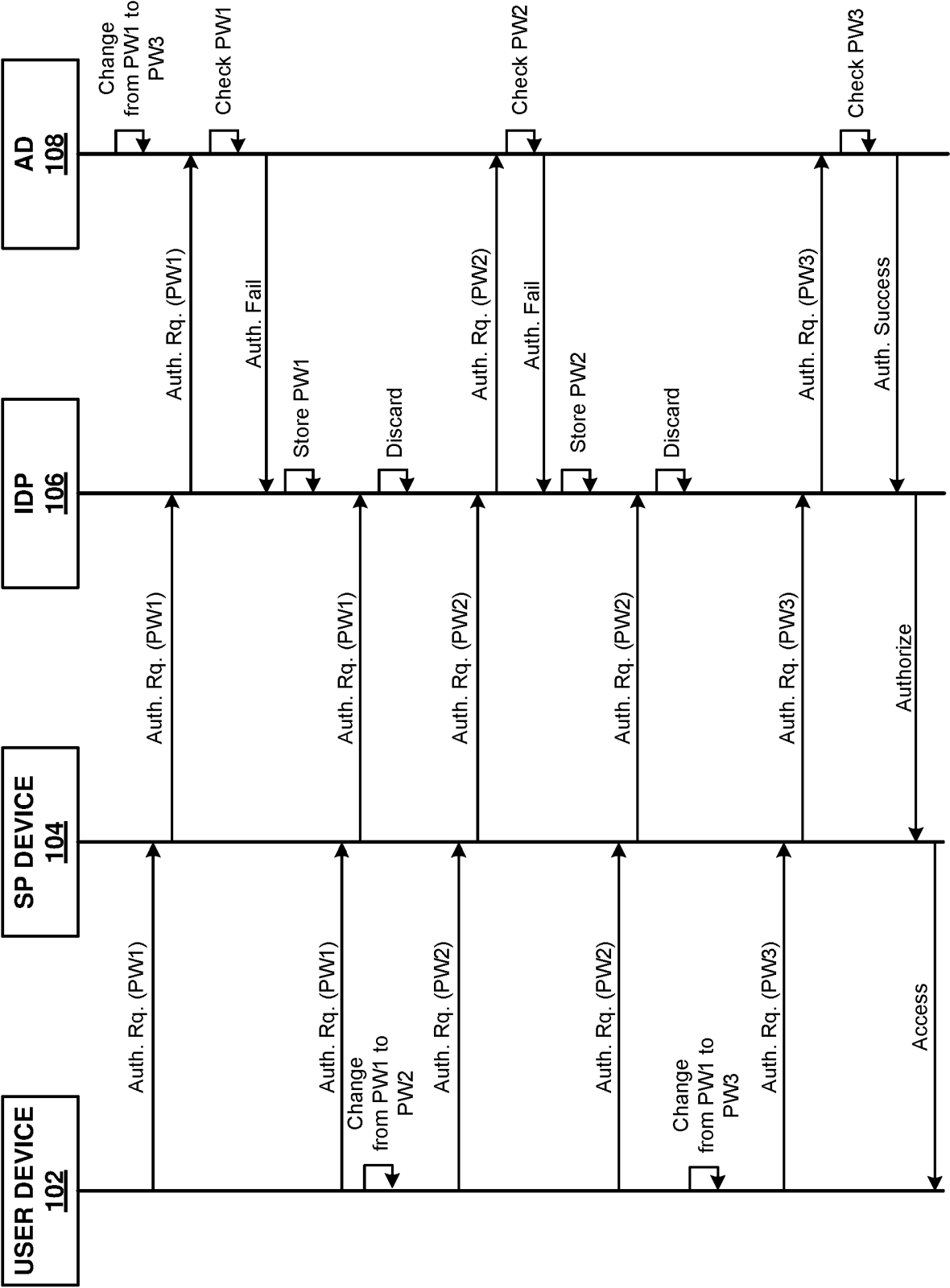


FIG. 3

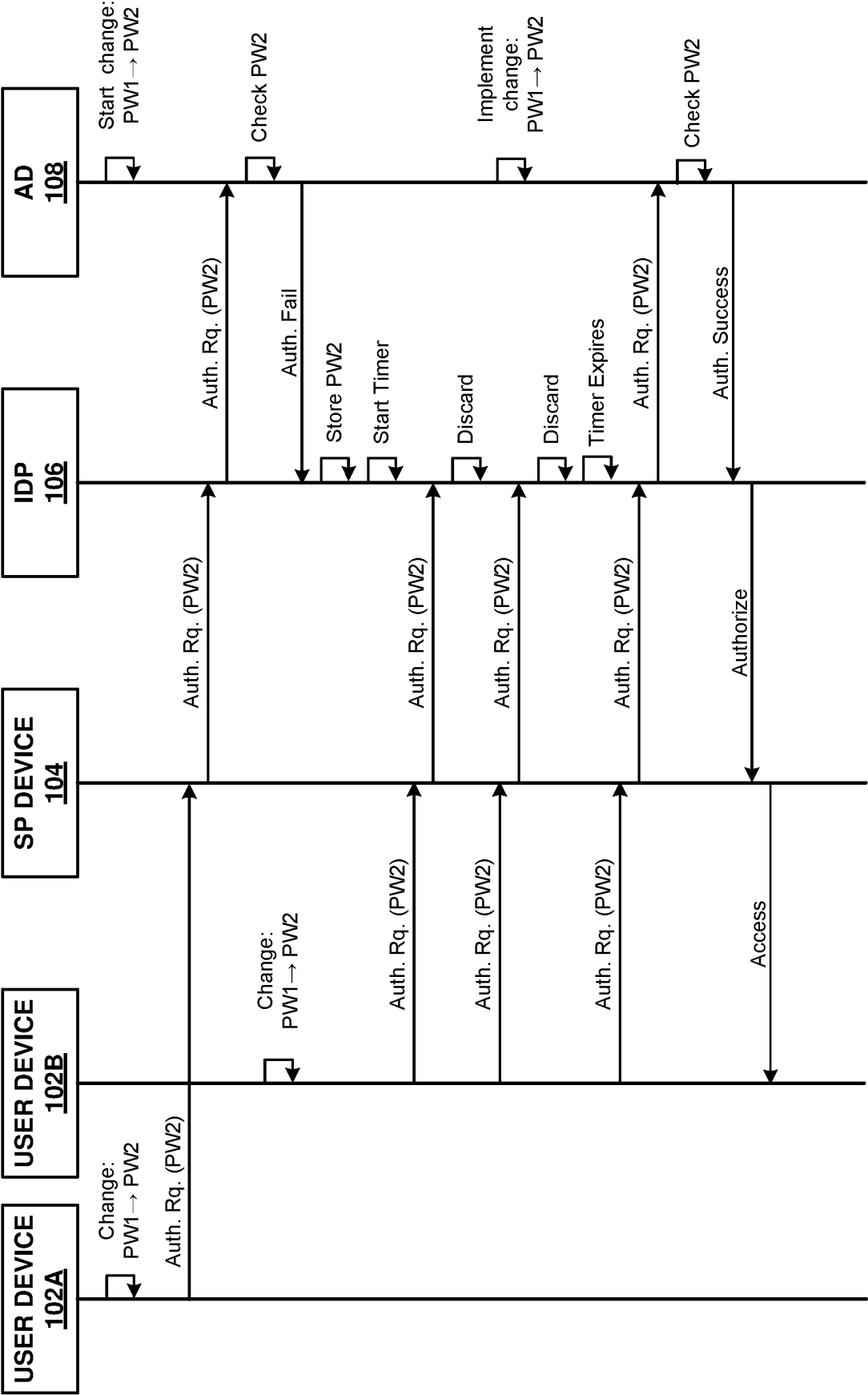


FIG. 4

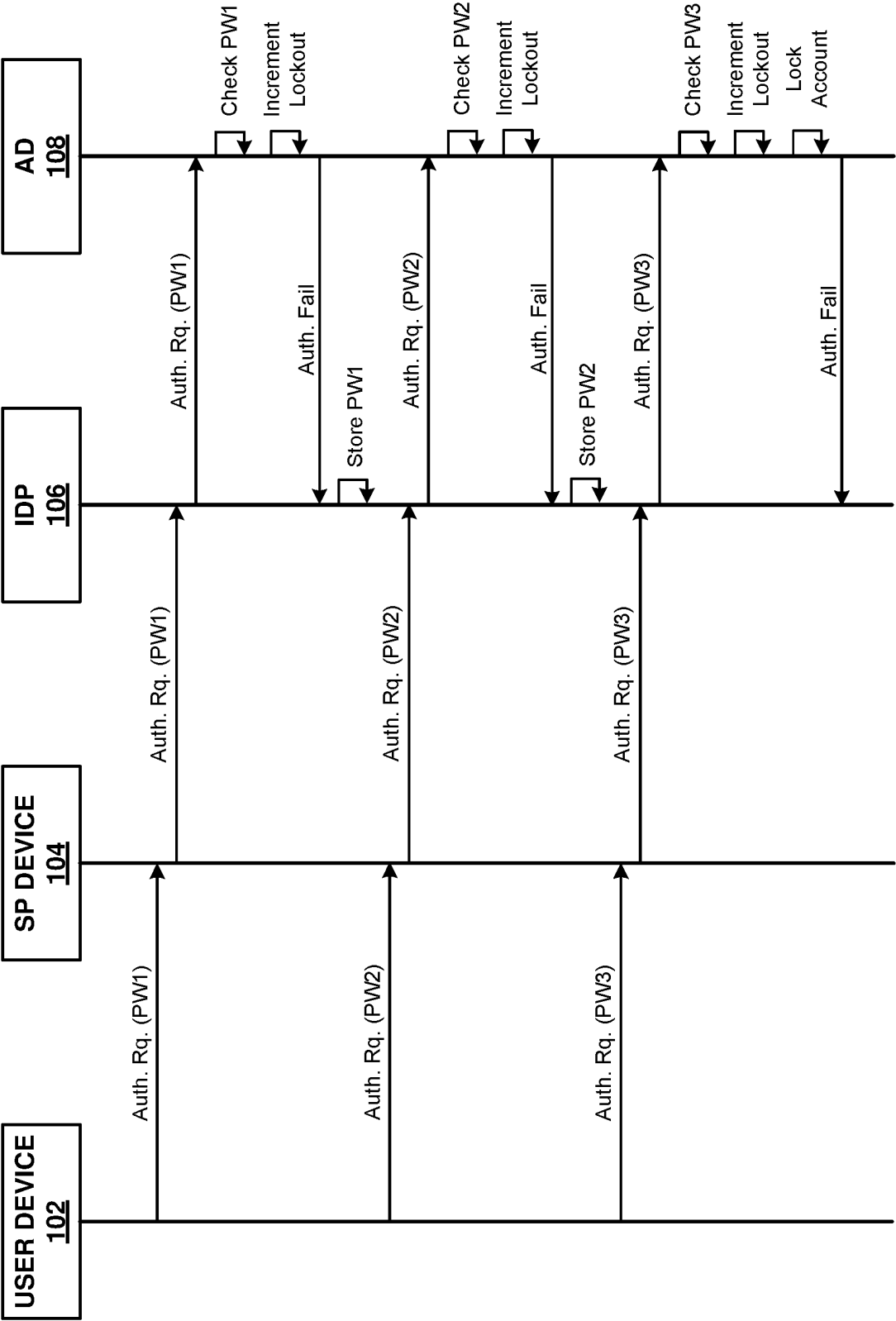


FIG. 5

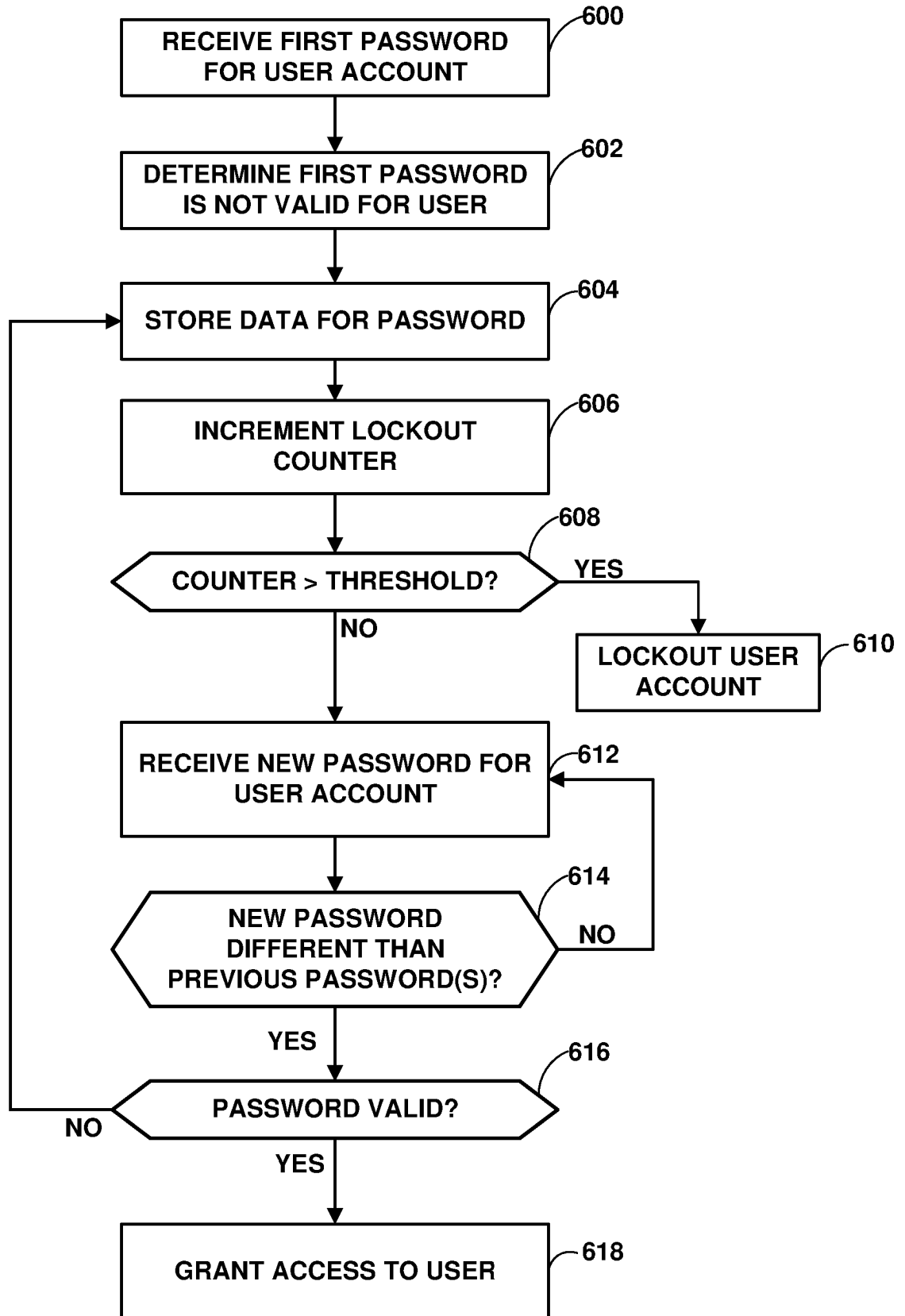


FIG. 6

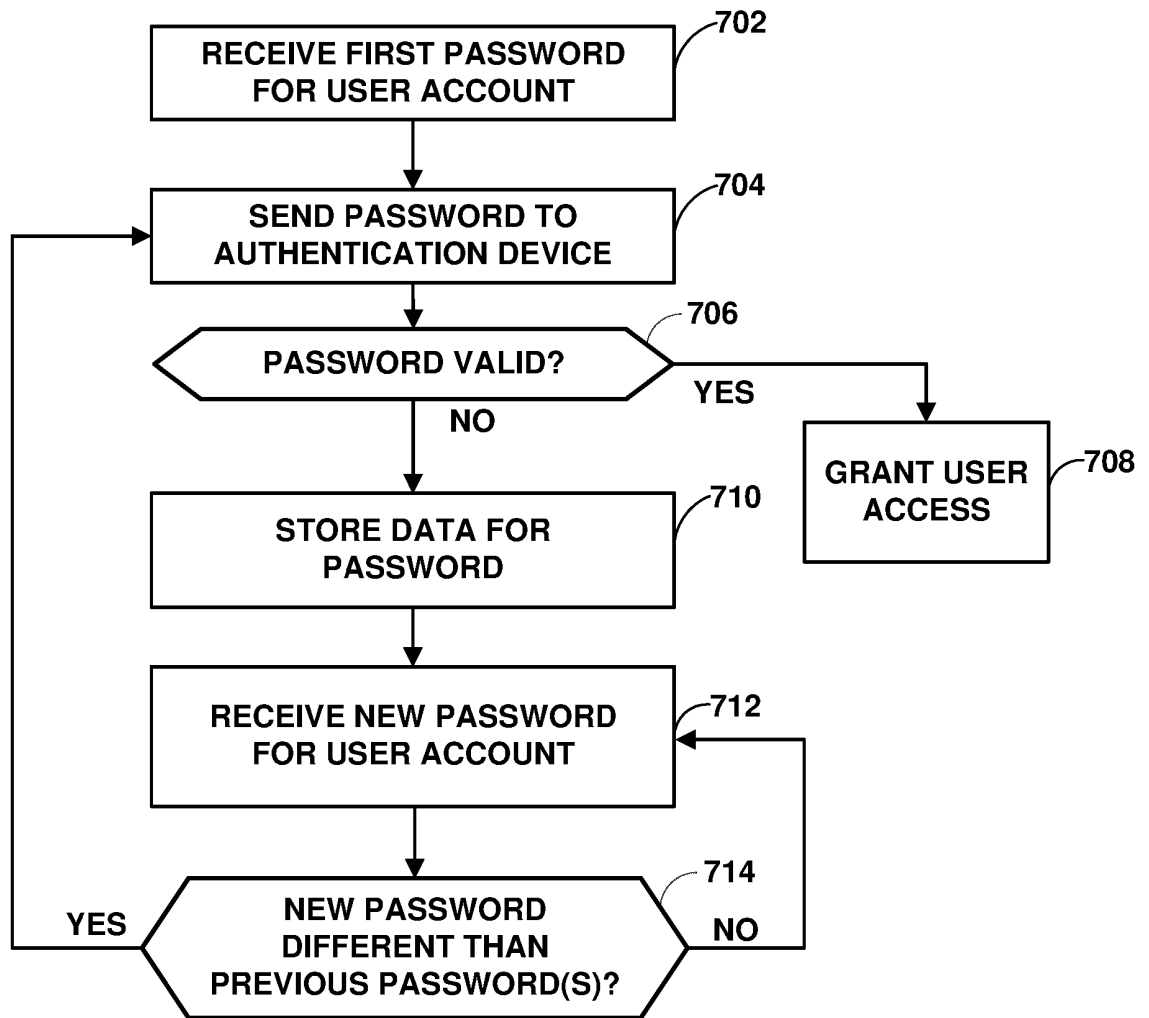


FIG. 7

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 62834274 [0001]
- US 2017208075 A1 [0007]
- US 2006130140 A1 [0008]
- US 2004093519 A1 [0009]